REMARKS

The Office Action dated January 8, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-3, 5, 6, 8-22, 26-30, 33, 35-41, and 44-47 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claim 49 has been added. No new matter has been added. Claims 1-49 are respectfully submitted for consideration.

Claims 1-5, 8-15, 19, 21, 22-26, 29, 31, 32, 34, 35-38, 42-44, 46, and 48 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 7,058,970 of Shaw (Shaw). It is respectfully submitted that the claims recite subject matter that is neither disclosed nor suggested in Shaw.

Independent claim 1, upon which claims 2-8 are dependent, recites an apparatus that includes a proxy configured to receive a request for network services by at least one remote network device and to perform a security integrity scanning operation on the requesting remote network device. The security scanning operation is performed at least before the network device signs on to the proxy. The apparatus also includes an authorization processor and access rules controller configured to determine if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

Independent claim 9, upon which claims 10-21 are dependent, recites a system that includes at least one remote network configured to access a network via a network connection to make a request for one or more network resident services. The system also includes a gateway configured to receive the request for services and perform a security integrity scanning operation on the remote network prior to allowing access to the requested network services, wherein the security scanning operation is performed at least before the remote network signs on to the gateway. The system includes an authentication server configured to verify user authentication credentials of users of remote network that access the network. The system includes at least one network server configured to provide requested network services to at least one remote network accessing the network through the gateway.

Independent claim 22, upon which claims 23-34 are dependent, recites a method that includes performing scanning process and reporting result used in scanning script, including at least one variable defined to be used as a vehicle to convey results of a scanning process. The method includes performing at least one scanning operation on the remote network device to verify a security integrity of the remote device, wherein the scanning operation is performed at least before the remote device signs on to a gateway device which is configured to perform the at least one scanning operation. The method includes providing the results of the scanning operation for purposes of determining whether or not the remote network device is authorized to access the requested network services.

Independent claim 35, upon which claims 36-48 are dependent, recites a method that includes defining at least one access control policy for accessing network services wherein the access control policy depends, at least in part, on the results of an integrity scan performed on a remote network device. The method includes specifying what scan scripts are to be used under what conditions to the remote network device. The method includes receiving at least one result of an integrity scan from the remote network device at a gateway device, wherein the integrity scan is performed at least before the remote device signs on to the gateway device. The method includes regulating access by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.

Independent claim 49 is an apparatus that includes proxying means for receiving a request for network services by at least one remote network device and to perform a security integrity scanning operation on the requesting remote network device, wherein the security scanning operation is performed at least before the remote network device signs on to the proxy. The apparatus also includes authorization processing means and access rules controlling means for determining if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

As will be discussed below, Shaw fails to disclose or suggest all of the elements of the presently pending claims.

Shaw generally describes a network security authority system that provides on-connect scan and delivery in a virtual lobby to enforce security requirements for a network. The client 808 starts outside the network and communicates with the on-connect security scan system 810. Then, the client's login is approved inside the virtual lobby. So, the client 808 does not get into the network at all if they do not have the correct user identification and password to login. If the client 808 is scanned and meets all the security requirements, then access is granted and the client 808 proceeds inside the network 806. See abstract and column 6, lines 53-61, of Shaw.

Applicants respectfully submit that Shaw fails to disclose or suggest, at least, "wherein the security scanning operation is performed at least before the remote network device signs on to the proxy," as recited in claim 1 and similarly recited in claims 9 and 22. The Office Action asserted that column 6, lines 53-61 of Shaw disclose the above-identified limitation. Applicants respectfully disagree. As discussed above, the cited portion describes that a security scanning operation is performed after the remote network device signs on to the proxy. Thus, Shaw fails to disclose or suggest, at least, "wherein the security scanning operation is performed at least before the remote network device signs on to the proxy," (Emphasis Added) as recited in the presently pending claims.

Therefore, Shaw does not disclose or suggest all of the features of independent claims 1, 9, 22, 35, and 49. Thus, it is respectfully requested that rejection of claims 1, 9, and 22 be withdrawn.

Claims 2-5, 8, 10-14, 19, 21, 23-26, 29, 31, 32, and 34 are dependent upon claims 1, 9, and 22. Thus, claims 2-5, 8, 10-14, 19, 21, 23-26, 29, 31, 32, and 34 should be allowed for at least their dependence upon claims 1, 9, and 22, and for the specific limitations recited therein.

Claims 6, 7, 16, 17, 27, 28, 40, and 41 were rejected under 35 U.S.C. 103(a) as being unpatentable over Shaw in view of U.S. Patent No. 6,728,886 of Ji et al. (Ji). The Office Action asserted that Shaw and Ji describe all of the features of claims 6, 7, 16, 17, 27, 28, 40, and 41. This rejection is respectfully traversed.

As discussed above, Shaw does not disclose or suggest all of the features of claims 1, 9, and 22. Ji does not cure the deficiencies in Shaw as failing to disclose or suggest, at least, "wherein the security scanning operation is performed at least before the remote network device signs on to the proxy." Thus, the combination of Shaw and Ji fails to disclose or suggest all of the elements of claims 1, 9, 22, and 35.

Claims 6, 7, 16, 17, 27, 28, 40, and 41 are dependent upon claims 1, 9, 22, and 35. Claims 6, 7, 16, 17, 27, 28, 40, and 41 should be allowed for at least their dependence upon claims 1, 9, 22, and 35, and for the specific limitations recited therein.

Claims 18, 20, 30, 33, 45, and 47 were rejected under 35 U.S.C. 103(a) as being unpatentable over Shaw in view of U.S. Patent Publication No. 2003/0177392 of Hiltgen (Hiltgen).

As discussed above, Shaw does not disclose or suggest all of the features of claims 1, 9, and 22. Hiltgen does not cure the deficiencies in Shaw as failing to disclose or

suggest, at least, "wherein the security scanning operation is performed at least before the remote network device signs on to the proxy." Thus, the combination of Shaw and Ji fails to disclose or suggest all of the elements of claims 1, 9, 22, and 35.

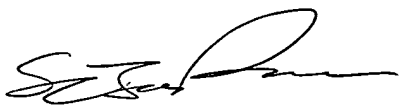
Claims 18, 20, 30, 33, 45, and 47 are dependent upon claims 1, 9, and 22. Claims 6, 7, 16, 17, 27, 28, 40, and 41 should be allowed for at least their dependence upon claims 1, 9, 22, and 35, and for the specific limitations recited therein.

For the reasons explained above, it is respectfully submitted that each of claims 1-49 recites subject matter that is neither disclosed nor suggested in the cited art. Also, it is respectfully submitted that the subject matter is more than sufficient to render the claimed invention unobvious to a person of ordinary skill in the art. It is, therefore, respectfully requested that all of claims 1-49 be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Sejoon Ahn
Registration No. 58,959

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

SA:dc

Enclosures: Petition for Extension of Time
Additional Claim Fee Transmittal
Check No. 18742